The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
9/14/2010

SUBJECT:
Vulnerability in Unicode Scripts Processor Could Allow Remote Code Execution (MS10-063)

OVERVIEW:
A vulnerability has been discovered in Microsoft Windows which could allow attackers to execute arbitrary code on the affected systems. The vulnerability is caused when Windows incorrectly parses specific font types. This may be exploited if a user opens a specially crafted document or web page viewed in an application which supports embedded OpenType fonts. OpenType is a modern font format developed by Adobe and Microsoft to provide users with an accessible and advanced typographic toolset. Successful exploitation of this vulnerability will result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:

- Windows XP
- Windows Server 2003
- Windows Vista
- Windows Server 2008

RISK:

Government:
- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

DESCRIPTION:
A vulnerability has been discovered in Microsoft Windows which could allow an attacker to execute arbitrary code on the affected systems. The vulnerability is caused when the Unicode Scripts Processor (usp10.DLL), also known as Uniscribe, incorrectly validates a table in the OpenType font layout. Uniscribe is the Microsoft Windows set of services for rendering Unicode-encoded text.

This vulnerability may be exploited if a user opens a specially crafted document or web page viewed in an application which supports embedded OpenType fonts. Successful exploitation will result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Consider applying workarounds contained in the Microsoft bulletin.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Remind users not to download or open files from un-trusted websites.

REFERENCES:

Microsoft:
http://www.microsoft.com/technet/security/bulletin/MS10-063.mspx

Securityfocus:
http://www.securityfocus.com/bid/43068

Secunia:
http://secunia.com/advisories/41396/

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2738